PAPER

Strongly Secure Privacy Amplification Cannot Be Obtained by Encoder of Slepian-Wolf Code*

Shun WATANABE[†a)], **Ryutaroh MATSUMOTO**[††b)], ***and*** **Tomohiko UYEMATSU**[††c)], ***Members***

SUMMARY The privacy amplification is a technique to distill a secret key from a random variable by a function so that the distilled key and eavesdropper's random variable are statistically independent. There are three kinds of security criteria for the key distilled by the privacy amplification: the normalized divergence criterion, which is also known as the weak security criterion, the variational distance criterion, and the divergence criterion, which is also known as the strong security criterion. As a technique to distill a secret key, it is known that the encoder of a Slepian-Wolf (the source coding with full side-information at the decoder) code can be used as a function for the privacy amplification if we employ the weak security criterion. In this paper, we show that the encoder of a Slepian-Wolf code cannot be used as a function for the privacy amplification if we employ the criteria other than the weak one.

key words: *privacy amplification, secret key agreement, Slepian-Wolf coding, strong security, variational distance, weak security*

1. Introduction

One of the fundamental problems in the cryptography is the key agreement in which the legitimate parties, usually referred to as Alice and Bob, share a secret key that is not known by the eavesdropper, usually referred to as Eve. The problems on the key agreement in the information theory was initiated by Maurer [11], and was also studied by Ahlswede and Csiszár [1]. In their formulation, Alice, Bob, and Eve have correlated random variables X^n, Y^n, and Z^n respectively. Then, Alice and Bob generate a secret key from (X^n, Y^n) by using the public (authenticated) communication.

Typically, a key agreement protocol consists of two procedures: the information reconciliation [3], [4] and the privacy amplification [2], [3]. The purpose of the information reconciliation for Alice and Bob is to share an identical random variable (with high probability) by using the public communication. The privacy amplification is a technique to distill a secret key from the shared random variable by using a function so that Eve's knowledge and the secret key are statistically independent. In order to focus on the privacy amplification, we assume that Alice and Bob initially share the random variables $X^n = Y^n$ in the rest of this paper.

As the security of the secret key distilled by the privacy amplification, there are three kinds of security criteria: the normalized divergence criterion, which is also known as the weak security criterion, the variational distance criterion, and the divergence criterion, which is also known as the strong security criterion. The normalized divergence criterion requires that the key and Eve's knowledge Z^n is (almost) statistically independent in the sense that the divergence divided by n (normalized divergence), or equivalently the mutual information divided by n, is negligible. On the other hand, the variational distance criterion and the divergence criterion require that the key and Eve's knowledge is (almost) statistically independent in the sense of the variational distance and the divergence are negligible respectively.

Traditionally, the normalized divergence criterion was employed in the study of the key agreement (e.g. [1], [11]). However, as Maurer and Wolf pointed out [12], Eve might know a large part of the key even if the key satisfies the normalized divergence criterion. Therefore, we should use the divergence criterion. Indeed, recent studies on the key agreement employ the divergence criterion (e.g. [7], [15]).

As one of techniques to distill a secret key, it is known that the encoder of a Slepian-Wolf (the source coding with full side-information at the decoder) code [19] can be used as a function for the privacy amplification. For example, Ahlswede and Csiszár used this technique implicitly [1], and Muramatsu used this technique explicitly [14].

To describe the technique more precisely, let us consider the Slepian-Wolf code system such that X^n is the principal source and Z^n is the side-information. Then, the output of the encoder, which is regarded as the key, satisfies the normalized divergence criterion if the coding rate of the code is close to the compression limit and the decoding error probability of the code is negligible. However, it has not been clarified whether this technique can be used for the divergence criterion.

Manuscript received June 5, 2009.
Manuscript revised June 6, 2009.
Final manuscript received June 7, 2009.

[†]The author is with the Department of Information Science and Intelligent Systems, Tokushima University

[††]The authors are with the Department of Communications and Integrated Sysmtems, Tokyo Institute of Technology

a) E-mail: shun-wata@is.tokushima-u.ac.jp
b) E-mail: ryutaroh@rmatsumoto.org
c) E-mail: uyematsu@ieee.org

*A part of this paper will be presented at 2009 IEEE International Symposium on Information Theory in Seoul, Korea.

In this paper, we show that above mentioned technique cannot be used for the divergence criterion. Actually, we show that the divergence grows infinitely in the order of $\sqrt{n}$, which suggests that Eve might know a large part of the key.

Although the divergence criterion is the strongest notion of security among the above mentioned three criteria, some researchers (eg. [18]) deem that the variational distance criterion is appropriate notion of security because it matches with the universally composable security [5], which requires that the actual distribution of the key and Eve's knowledge is indistinguishable from the ideal distribution with which the key is uniformly distributed and independent of Eve's knowledge. Therefore, it is worthwhile clarifying whether the key obtained by the above mentioned technique satisfies the variational distance criterion or not. In this paper, we show that the key obtained by the technique does not satisfy the variational distance criterion. Actually, we show that the variational distance converges to one (the maximum amount), which means that the actual distribution and the ideal distribution is completely distinguishable.

The results in this paper are also interesting from the view point other than the privacy amplification. The above mentioned technique can be regarded as the Slepian-Wolf version of the folklore theorem shown by Han [9]. Recently, Hayashi [10] showed that the folklore theorem does not hold if we employ the variational distance criterion nor the divergence criterion instead of the normalized divergence criterion. Our results can be regarded as a generalization of Hayashi's results for the Slepian-Wolf code.

The rest of this paper is organized as follows: In Section 2, we review the basic notations, the privacy amplification, and the above mentioned technique. In Section 3, we show our main results concerning the divergence criterion and their proofs. In Section 4, we show our main results concerning the variational distance criterion and their proofs. In Section 5, we conclude the paper.

Finally, it should be noted that the results on the divergence criterion and the variational distance criterion cannot be derived from each other, though a weak version of the result on the divergence criterion, i.e., the fact that the divergence does not converge to zero (Corollary 12), can be derived as a corollary of the results on the variational distance criterion. The weak version only suggests that Eve might know a few bits about the key whose length grows infinitely as n goes to infinite, which is not a serious problem in practice. On the other hand, the result in Section 3 suggests that Eve's knowledge about the key also grows infinitely as the length of the key goes to infinite, which is a serious problem in practice. Therefore, we need to treat both the divergence criterion and the variational distance criterion separately.

2. Preliminaries

2.1 Privacy Amplification

In this section, we review the basic notations related to the privacy amplification. Suppose that Alice and Bob have a random variable X^n on $\mathcal{X}^n$, and Eve has a random variable Z^n on $\mathcal{Z}^n$, where (X^n, Z^n) are independently identically distributed (i.i.d.) according to the probability distribution P_{XZ}. In this paper, we assume that $\mathcal{X}$ and $\mathcal{Z}$ are finite sets.

The privacy amplification [2], [3] is a technique to distill a secret key S_n from X^n by using a function

$$f_n : \mathcal{X}^n \to \mathcal{M}_n = \{1, \ldots, M_n\}$$

so that the key and Eve's information Z^n are statistically independent and the key is uniformly distributed on the key alphabet $\mathcal{M}_n$. The joint probability distribution of the key and Eve's information is given by

$$P_{S_n Z^n}(s, z^n) = \sum_{x^n \in f_n^{-1}(s)} P_{X^n Z^n}(x^n, z^n) \tag{1}$$

for $(s, z^n) \in \mathcal{M}_n \times \mathcal{Z}^n$, where we defined $f_n^{-1}(s) = \{x^n : f_n(x^n) = s\}$.

For probability distributions P and Q on $\mathcal{A}$, let

$$d(P, Q) = \frac{1}{2} \sum_{a \in \mathcal{A}} |P(a) - Q(a)|$$

be the variational distance (divided by 2), and let

$$D(P\|Q) = \sum_{a \in \mathcal{A}} P(a) \log \frac{P(a)}{Q(a)}$$

be the divergence respectively [6], where we take the base of the logarithm to be e throughout the paper. By using these two quantities, we introduce three kinds of security criteria on the privacy amplification.

Definition 1 If a sequence of functions $\{f_n\}$ satisfies

$$\lim_{n \to \infty} \frac{1}{n} D(f_n) = 0 \tag{2}$$

for

$$D(f_n) = D(P_{S_n Z^n} \| P_{U_n} \times P_{Z^n}),$$

then we define the privacy amplification by $\{f_n\}$ to be secure with respect to the *normalized divergence criterion*, where P_{U_n} is the uniform distribution on $\mathcal{M}_n$.

Definition 2 If a sequence of functions $\{f_n\}$ satisfies

$$\lim_{n \to \infty} \Delta(f_n) = 0 \tag{3}$$

for

$$\Delta(f_n) = d(P_{S_n Z^n}, P_U \times P_{Z^n}),$$

then we define the privacy amplification by $\{f_n\}$ to be secure with respect to the *variational distance criterion*.

Definition 3 If a sequence of functions $\{f_n\}$ satisfies

$$\lim_{n\to\infty} D(f_n) = 0, \tag{4}$$

then we define the privacy amplification by $\{f_n\}$ to be secure with respect to the *divergence criterion*.

We can show that Eq. (4) implies Eq. (3) by using Pinsker's inequality [6]. We can also show that Eq. (3) implies Eq. (2) by using [7, Lemma 1].

The security criteria in Definitions 1 and 3 are equivalent to the weak security criterion and the strong security criterion defined in [12]. The security criterion in Definition 2 is widely used recently (eg. [18]) because it match with the universally composable security [5], which requires that the actual distribution $P_{S_n Z^n}$ and the ideal distribution $P_{U_n} \times P_{Z^n}$ are indistinguishable. Although the divergence is also related to the distinguishability between distributions, the variational distance is directly related to the distinguishability because the optimized average probability of the correct discrimination is given by

$$\begin{aligned}&\frac{1}{2}\max_{\mathcal{A}\subset\mathcal{M}_n\times\mathcal{Z}^n}[P_{S_n Z^n}(\mathcal{A}) + P_{U_n Z^n}(\mathcal{A}^c)]\\ &= \frac{1}{2}[1 + d(P_{S_n Z^n}, P_{U_n}\times P_{Z^n})],\end{aligned} \tag{5}$$

which is a straightforward consequence of the definition of the variational distance [6], where the superscript c designate the complement of the set.

2.2 Privacy Amplification by an Encoder of Slepian-Wolf Code

In this section, we explain the Slepian-Wolf code, and then review the relation between the privacy amplification and the Slepian-Wolf code. We consider the Slepian-Wolf code system in which X^n is the principal source and Z^n is the side-information. The code system consists of the encoder

$$\phi_n : \mathcal{X}^n \to \mathcal{M}_n$$

and the decoder

$$\psi_n : \mathcal{M}_n \times \mathcal{Z}^n \to \mathcal{X}^n,$$

and we denote the code as $\Phi_n = (\phi_n, \psi_n)$. The error probability of the code is defined as

$$\varepsilon(\Phi_n) = P_{X^n Z^n}(\{(x^n, z^n) : \ \psi_n(\phi_n(x^n), z^n) \neq x^n\}).$$

For any real number $R > 0$, we call the rate R is achievable if there exists a sequence of codes $\{\Phi_n\}$ that satisfies

$$\limsup_{n\to\infty} \frac{1}{n}\log M_n \le R \ \text{ and } \ \lim_{n\to\infty}\varepsilon(\Phi_n) = 0.$$

Then, we define the compression limit as

$$R_f(X|Z) = \inf\{R : \ R \text{ is achievable}\}.$$

It is well known that the compression limit coincide with the conditional entropy [19], i.e., $R_f(X|Z) = H(X|Z)$.

If a sequence of code $\{\Phi_n\}$ satisfies

$$\lim_{n\to\infty}\frac{1}{n}\log M_n = H(X|Z) \tag{6}$$

and

$$\lim_{n\to\infty}\varepsilon(\Phi_n) = 0, \tag{7}$$

then we call the sequence of codes $\{\Phi_n\}$ *compression limit achieving codes*. When $\{\Phi_n\}$ satisfies Eq. (6), it should be noted that the error probability depends on the second order rate $\frac{1}{\sqrt{n}}\log\frac{M_n}{e^{nH(X|Z)}}$. For later use, we present the converse coding theorem concerning the tradeoff between the error probability and the second order rate. The theorem is a Slepian-Wolf coding version of the result on the second order asymptotic of the source coding [10].

Theorem 4 Let $b \in \mathbb{R}$ be arbitrary real number. For any code sequence $\{\Phi_n\}$, if the error probability satisfies

$$\limsup_{n\to\infty}\varepsilon(\Phi_n) < 1 - G\left(\frac{b}{\sigma}\right), \tag{8}$$

then the rate satisfies

$$\liminf_{n\to\infty}\frac{1}{\sqrt{n}}\log\frac{M_n}{e^{nH(X|Z)}} \ge b, \tag{9}$$

where

$$G(t) = \int_{-\infty}^{t}\frac{1}{\sqrt{2\pi}}e^{-u^2/2}du$$

is the cumulative distribution function of the Gaussian distribution with mean 0 and variance 1, and where we set

$$\sigma^2 = \mathrm{Var}\left[\log\frac{1}{P_{X|Z}(X|Z)}\right]. \tag{10}$$

This theorem is a straight forward consequence of the central limit theorem, and we show a proof in Appendix A.

The following proposition states that the encoders of compression limit achieving codes can be used as functions for the privacy amplification if we employ the normalized divergence criterion.

Proposition 5 If a sequence of code $\{\Phi_n = (\phi_n, \psi_n)\}$ satisfies Eqs. (6) and (7), then we have

$$\lim_{n\to\infty}\frac{1}{n}D(\phi_n) = 0.$$

This proposition can be proved almost in a similar manner to [14, Theorem 1]. Note that Proposition 5 can be regarded as the Slepian-Wolf version of the folklore theorem [9] (see also [8, Theorem 2.6.4]).

3. Divergence Criterion

3.1 Statement of Results

In this section, we show our main results concerning the divergence criterion, which are proved in Section 3.2. In Section 2.2, we showed that the encoders of compression limit achieving codes can be used as functions for the privacy amplification which is secure in the sense of the normalized divergence criterion. The following theorem states that the divergence actually grows infinitely in the order of $\sqrt{n}$ (Eq. (12)), which suggest that Eve might know a large part of the key. The following theorem can be regarded as a generalization of [10, Theorem 8] for the Slepian-Wolf code.

Theorem 6 Suppose that a sequence of functions, $f_n : \mathcal{X}^n \to \{1, \ldots, M_n\}$ for $n = 1, 2, \ldots$, satisfies Eq. (6), and let

$$b = \liminf_{n\to\infty} \frac{1}{\sqrt{n}} \log \frac{M_n}{e^{nH(X|Z)}}.$$

Then, we have

$$\liminf_{n\to\infty} \frac{1}{\sqrt{n}} D(f_n) \geq \int_{-\infty}^{\frac{b}{\sigma}} (b - \sigma u) g(u) du, \tag{11}$$

where

$$g(u) = \frac{1}{\sqrt{2\pi}} e^{-u^2/2}$$

is the density function of the Gaussian distribution with mean 0 and variance 1, and where σ^2 is the variance defined in Eq. (10).

Suppose that the Slepian-Wolf code sequence $\{\Phi_n = (\phi_n, \psi_n)\}$ satisfies Eq. (6) and

$$\limsup_{n\to\infty} \varepsilon(\Phi_n) < 1.$$

Then, there exist a real number $b \in \mathbb{R}$ such that

$$\limsup_{n\to\infty} \varepsilon(\Phi_n) < 1 - G\left(\frac{b}{\sigma}\right).$$

Since the right hand side of Eq. (11) is an increasing function of b and is positive for any $b \in \mathbb{R}$, Theorem 4 and Theorem 6 imply that there exists a constant $K > 0$ and an integer n_0 such that

$$D(\phi_n) \geq \sqrt{n} K \tag{12}$$

for every $n \geq n_0$.

3.2 Proof of Theorem 6

In order to show a proof of Theorem 6, we need the following lemma.

Lemma 7 Let

$$\mathcal{T}_n = \left\{ (x^n, z^n) : \frac{1}{\sigma\sqrt{n}} \left(\log \frac{1}{P_{X^n|Z^n}(x^n|z^n)} - nH(X|Z) \right) \leq \frac{b}{\sigma} \right\}.$$

Then, we have

$$\begin{aligned} &H(S_n|Z^n) \\ &\leq \sum_{(x^n,z^n)\in\mathcal{T}_n} P_{X^nZ^n}(x^n, z^n) \log \frac{1}{P_{X^n|Z^n}(x^n|z^n)} \\ &\quad + P_{X^nZ^n}(\mathcal{T}_n^c)[\log M_n - \log P_{X^nZ^n}(\mathcal{T}_n^c)]. \end{aligned}$$

Proof. Let

$$\mathcal{M}'_n = \mathcal{M}_n \cup \mathcal{X}^n,$$

and let $f'_n : \mathcal{X}^n \times \mathcal{Z}^n \to \mathcal{M}'_n$ be the function defined by

$$f'_n(x^n, z^n) = \begin{cases} f_n(x^n) & \text{if } (x^n, z^n) \notin \mathcal{T}_n \\ x^n & \text{if } (x^n, z^n) \in \mathcal{T}_n \end{cases}.$$

We set the random variable $S'_n = f'_n(X^n, Z^n)$. Then, we have

$$\begin{aligned} &H(S'_n|Z^n) \\ &= \sum_{(x^n,z^n)\in\mathcal{T}_n} P_{X^nZ^n}(x^n, z^n) \log \frac{1}{P_{X^n|Z^n}(x^n|z^n)} \\ &\quad + \sum_{(s,z^n)\in\mathcal{M}_n\times\mathcal{Z}^n} P_{S'_nZ^n}(s, z^n) \log \frac{1}{P_{S'_n|Z^n}(s|z^n)}. \end{aligned} \tag{13}$$

By using the log-sum inequality [6], we can upper bound the last term in Eq. (13) as

$$\begin{aligned} &\sum_{(s,z^n)\in\mathcal{M}_n\times\mathcal{Z}^n} P_{S'_nZ^n}(s, z^n) \log \frac{P_{Z^n}(z^n)}{P_{S'_nZ^n}(s, z^n)} \\ &\leq P_{X^nZ^n}(\mathcal{T}_n^c)[\log M_n - \log P_{X^nZ^n}(\mathcal{T}_n^c)]. \end{aligned} \tag{14}$$

Let $f''_n : \mathcal{M}'_n \to \mathcal{M}_n$ be the function defined by

$$f''_n(s) = \begin{cases} s & \text{if } s \in \mathcal{M}_n \\ f_n(s) & \text{if } s \in \mathcal{X}^n \end{cases}.$$

Then, we have $S_n = f''_n(S'_n)$. Since the conditional entropy does not increase by a function [6], by combining Eqs. (13) and (14), we have the assertion of the lemma. □

Proof of Theorem 6

By using Lemma 7, we have

$$
\begin{aligned}
&\frac{1}{\sqrt{n}}D(f_n)\\
&= \frac{1}{\sqrt{n}}\left[\log\frac{M_n}{e^{nH(X|Z)}} - (H(S_n|Z^n) - nH(X|Z))\right]\\
&\geq P_{X^nZ^n}(\mathcal{T}_n)\frac{1}{\sqrt{n}}\log\frac{M_n}{e^{nH(X|Z)}}\\
&\quad -\sigma\sum_{(x^n,z^n)\in\mathcal{T}_n} P_{X^nZ^n}(x^n,z^n)\\
&\quad \frac{1}{\sigma\sqrt{n}}\left(\log\frac{1}{P_{X^n|Z^n}(x^n|z^n)} - nH(X|Z)\right)\\
&\quad +\frac{1}{\sqrt{n}}P_{X^nZ^n}(\mathcal{T}_n^c)\log P_{X^nZ^n}(\mathcal{T}_n^c).
\end{aligned}
$$

By taking the limit of both side and using the central limit theorem with respect to the cumulative distribution function

$$
\Pr\left\{\frac{1}{\sigma\sqrt{n}}\left(\log\frac{1}{P_{X^n|Z^n}(X^n|Z^n)} - nH(X|Z)\right)\leq u\right\},
$$

we have

$$
\begin{aligned}
&\liminf_{n\to\infty}\frac{1}{\sqrt{n}}D(f_n)\\
&\geq bG\left(\frac{b}{\sigma}\right) - \sigma\int_{-\infty}^{\frac{b}{\sigma}} ug(u)du\\
&= \int_{-\infty}^{\frac{b}{\sigma}}(b-\sigma u)g(u)du,
\end{aligned}
$$

which completes the proof □

4. Variational Distance Criterion

4.1 Statement of Results

In this section, we show our main results concerning the variational distance criterion, which are proved in Sections 4.2 and 4.3 respectively. First, we define the quantity $\delta(P_{X^nZ^n})$ as follows.

Definition 8 Let $1 \leq M_n \leq |\mathcal{X}|^n$ be an integer, and $\mathcal{C}_n = \{\mathcal{C}_{z^n}\}_{z^n\in\mathcal{Z}^n}$ be a family of sets such that each $\mathcal{C}_{z^n} \subset \mathcal{X}^n$ satisfies $|\mathcal{C}_{z^n}| = M_n$, where $|\mathcal{A}|$ means the cardinality of a set $\mathcal{A}$. We define the distribution $P_{\mathcal{C}_n}$ on $\mathcal{X}^n \times \mathcal{Z}^n$ as

$$
P_{\mathcal{C}_n}(x^n,z^n) = \begin{cases} \frac{1}{M_n}P_{Z^n}(z^n) & \text{if } x^n \in \mathcal{C}_{z^n}\\ 0 & \text{else}\end{cases}.
$$

Then, we define

$$
\delta(P_{X^nZ^n}) = \min_{\mathcal{C}_n} d(P_{X^nZ^n}, P_{\mathcal{C}_n}), \tag{15}
$$

where the minimization is taken over all possible choice of $\mathcal{C}_n$ for arbitrary $1 \leq M_n \leq |\mathcal{X}|^n$.

In Section 2.2, we showed that the encoders of compression limit achieving codes can be used as functions for the privacy amplification which is secure in the sense of the normalized divergence criterion. However, the following Theorem 9 shows a trade-off (with some exceptions) between the error probability $\varepsilon(\Phi_n)$ and the security parameter $\Delta(\phi_n)$ for any code Φ_n. Then, the combination of Theorems 9 and 10 states that we cannot use the encoders of any (good) Slepian-Wolf codes as functions for the secure privacy amplification if we employ the variational distance criterion.

Theorem 9 For arbitrary Slepian-Wolf code $\Phi_n = (\phi_n, \psi_n)$, we have

$$
\varepsilon(\Phi_n) + \Delta(\phi_n) \geq \delta(P_{X^nZ^n}).
$$

Theorem 10 If the variance σ^2 defined in Eq. (10) is positive, then we have

$$
\lim_{n\to\infty}\delta(P_{X^nZ^n}) = 1. \tag{16}
$$

Corollary 11 For arbitrary Slepian-Wolf code $\Phi_n = (\phi_n, \psi_n)$, if

$$
\lim_{n\to\infty}\varepsilon(\Phi_n) = 0,
$$

then we have

$$
\lim_{n\to\infty}\Delta(\phi_n) = 1
$$

provided that $\sigma^2 > 0$. □

From Eq. (5), Corollary 11 means that the actual distribution $P_{S_nZ^n}$ and the ideal distribution $P_{U_n} \times P_{Z^n}$ are completely distinguishable asymptotically.

The combination of Pinsker's inequality and Corollary 11 imply the following corollary, which states that the keys obtained by the encoders of any (good) Slepian-Wolf codes do not satisfy the divergence criterion, although we have shown stronger result in Section 3. The following corollary only suggests that Eve might know a few bits about the long key, which is not a serious problem in practice. On the other hand, the stronger result suggests that Eve's knowledge about the key grows infinitely as the length of the key goes to infinite, which is a serious problem in practice.

Corollary 12 For any sequence of Slepian-Wolf codes $\{\Phi_n = (\phi_n, \psi_n)\}$ such that $\lim_{n\to\infty}\varepsilon(\Phi_n) = 0$, we have

$$
\liminf_{n\to\infty} D(\phi_n) \geq \frac{2}{\ln 2}
$$

provided that $\sigma^2 > 0$. □

Theorems 9 and 10 can be regarded as a generalization of [10, Theorem 4] for the Slepian-Wolf code. Therefore, we can also interpret Theorems 9 and 10 as follows: The Slepian-Wolf version of the folklore theorem does not hold for the variational distance criterion.

Remark 13 For a distribution P_{XZ} with $\sigma = 0$, we can easily show that $\delta(P_{X^nZ^n}) = 0$ for any n by taking $\mathcal{C}_{z^n}$ as the support of $P_{X^n|Z^n}(x^n|z^n)$.

Remark 14 It should be noted that Theorem 9 holds not only for i.i.d. random variables (X^n, Z^n), but also for any (X^n, Z^n).

4.2 Proof of Theorem 9

Before we show a proof of Theorem 9, we introduce the following lemma.

Lemma 15 For arbitrary code $\Phi_n = (\phi_n, \psi_n)$, there exists a code $\Phi'_n = (\phi_n, \psi'_n)$ that satisfies

$$\varepsilon(\Phi'_n) \le \varepsilon(\Phi_n) \tag{17}$$

and

$$\phi_n(\psi'_n(s, z^n)) = s \quad \forall (s, z^n) \in \mathcal{M}_n \times \mathcal{Z}^n. \tag{18}$$

Proof. We construct a decoder ψ'_n as follows. If $\phi_n(\psi_n(s, z^n)) \neq s$, then we set $\psi'_n(s, z^n) = \tilde{x}^n$ for arbitrarily chosen $\tilde{x}^n \in \phi_n^{-1}(s)$. Otherwise, we set $\psi'_n(s, z^n) = \psi_n(s, z^n)$. From the construction of this decoder, it is obvious that the code $\Phi'_n = (\phi_n, \psi'_n)$ satisfies Eqs. (17) and (18). □

Proof of Theorem 9

From Lemma 15, it suffice to prove Theorem 9 for codes satisfying Eq. (18). Therefore, we assume that a code Φ_n satisfies Eq. (18) in the rest of this section.

By using the decoder ψ_n, we construct the map

$$\overline{\psi}_n(s, z^n) = (\psi_n(s, z^n), z^n). \tag{19}$$

Since the decoder satisfies the condition in Eq. (18), $\overline{\psi}_n$ is an injection map from $\mathcal{M}_n \times \mathcal{Z}^n$ into $\mathcal{X}^n \times \mathcal{Z}^n$.

For the extended code $\overline{\Phi}_n = (\phi_n, \overline{\psi}_n)$, we define the error probability

$$\begin{aligned}&\varepsilon(\overline{\Phi}_n)\\ &= P_{X^nZ^n}(\{(x^n, z^n) : \overline{\psi}_n(\phi_n(x^n), z^n) \neq (x^n, z^n)\}).\end{aligned}$$

Obviously, we have $\varepsilon(\overline{\Phi}_n) = \varepsilon(\Phi_n)$.

Next, we define the distribution $\overline{P_{U_n} \times P_{Z^n}}$, which is the embedding of $P_{U_n} \times P_{Z^n}$ into $\mathcal{X}^n \times \mathcal{Z}^n$, as follows:

$$\overline{P_{U_n} \times P_{Z^n}}(x^n, z^n) = P_{U_n} \times P_{Z^n}(\overline{\psi}_n^{-1}(x^n, z^n))$$

for $(x^n, z^n) \in \overline{\psi}_n(\mathcal{M}_n \times \mathcal{Z}^n)$, and $\overline{P_{U_n} \times P_{Z^n}}(x^n, z^n) = 0$ for other (x^n, z^n). Similarly, we define the distribution $\overline{P_{S_nZ^n}}$, which is the embedding of $P_{S_nZ^n}$ into $\mathcal{X}^n \times \mathcal{Z}^n$.

Since the decoder ψ_n satisfies Eq. (18), we have

$$\begin{aligned}P_{X^nZ^n}(\overline{\psi}_n(s, z^n)) &\le \sum_{x^n \in \phi_n^{-1}(s)} P_{X^nZ^n}(x^n, z^n)\\ &= \overline{P_{S_nZ^n}}(\overline{\psi}_n(s, z^n))\end{aligned} \tag{20}$$

for $(s, z^n) \in \mathcal{M}_n \times \mathcal{Z}^n$, where the equality in Eq. (20) follows from Eq. (1) and the definition of $\overline{P_{S_nZ^n}}$. On the other hand, we have

$$P_{X^nZ^n}(x^n, z^n) \ge \overline{P_{S_nZ^n}}(x^n, z^n) = 0 \tag{21}$$

for $(x^n, z^n) \in (\mathcal{X}^n \times \mathcal{Z}^n) \backslash \overline{\psi}_n(\mathcal{M}_n \times \mathcal{Z}^n)$. Combining Eqs. (20) and (21), we have

$$\begin{aligned}&d(P_{X^nZ^n}, \overline{P_{S_nZ^n}})\\ &= P_{X^nZ^n}((\mathcal{X}^n \times \mathcal{Z}^n) \backslash \overline{\psi}_n(\mathcal{M}_n \times \mathcal{Z}^n)).\end{aligned} \tag{22}$$

By using Eq. (22), we can rewrite $\varepsilon(\overline{\Phi}_n)$ as

$$\begin{aligned}\varepsilon(\overline{\Phi}_n) &= P_{X^nZ^n}((\mathcal{X}^n \times \mathcal{Z}^n) \backslash \overline{\psi}_n(\mathcal{M}_n \times \mathcal{Z}^n))\\ &= d(P_{X^nZ^n}, \overline{P_{S_nZ^n}}).\end{aligned}$$

Finally, from the definition of $\delta(P_{X^nZ^n})$ and the triangular inequality, we have

$$\begin{aligned}\delta(P_{X^nZ^n}) &\le d(P_{X^nZ^n}, \overline{P_{U_n} \times P_{Z^n}})\\ &\le d(P_{X^nZ^n}, \overline{P_{S_nZ^n}})\\ &\quad + d(\overline{P_{S_nZ^n}}, \overline{P_{U_n} \times P_{Z^n}})\\ &= \varepsilon(\Phi_n) + \Delta(\phi_n),\end{aligned}$$

which completes the proof of Theorem 9. □

4.3 Proof of Theorem 10

Let $\{\mathcal{C}_n\}$ be the sequence of the families such that $d(P_{X^nZ^n}, P_{\mathcal{C}_n}) = \delta(P_{X^nZ^n})$ for each n. For arbitrary positive constant $b > 0$, we divide $\mathcal{X}^n \times \mathcal{Z}^n$ into the following three subsets:

$$\begin{aligned}\mathcal{A}_+ &= \{(x^n, z^n) : M_n^{-1} e^{b\sqrt{n}} < P_{X^n|Z^n}(x^n|z^n)\},\\ \mathcal{A}_- &= \{(x^n, z^n) : P_{X^n|Z^n}(x^n|z^n) \le M_n^{-1} e^{-b\sqrt{n}}\},\end{aligned}$$

and $\mathcal{A}_0 = (\mathcal{X}^n \times \mathcal{Z}^n) \backslash (\mathcal{A}_+ \cup \mathcal{A}_-)$. Let

$$\overline{\mathcal{C}}_n = \bigcup_{z^n \in \mathcal{Z}^n} \{(x^n, z^n) : x^n \in \mathcal{C}_{z^n}\},$$

which is the support of $P_{\mathcal{C}_n}$.

We bound $\delta(P_{X^nZ^n})$ as follows:

$$\begin{aligned}&\delta(P_{X^nZ^n})\\ &= \frac{1}{2}\left[\sum_{(x^n,z^n)\in\mathcal{A}_+} |P_{X^nZ^n}(x^n, z^n) - P_{\mathcal{C}_n}(x^n, z^n)|\right.\\ &\quad + \sum_{(x^n,z^n)\in\mathcal{A}_-} |P_{X^nZ^n}(x^n, z^n) - P_{\mathcal{C}_n}(x^n, z^n)|\\ &\quad \left. + \sum_{(x^n,z^n)\in\mathcal{A}_0} |P_{X^nZ^n}(x^n, z^n) - P_{\mathcal{C}_n}(x^n, z^n)|\right]\\ &\ge \frac{1}{2}[(P_{X^nZ^n}(\mathcal{A}_+) - P_{\mathcal{C}_n}(\mathcal{A}_+))\\ &\quad + (P_{\mathcal{C}_n}(\mathcal{A}_-) - P_{X^nZ^n}(\mathcal{A}_- \cap \overline{\mathcal{C}}_n)\\ &\quad + P_{X^nZ^n}(\mathcal{A}_- \backslash \overline{\mathcal{C}}_n))\\ &\quad + (P_{\mathcal{C}_n}(\mathcal{A}_0) - P_{X^nZ^n}(\mathcal{A}_0))]\\ &= 1 - (P_{\mathcal{C}_n}(\mathcal{A}_+) + P_{X^nZ^n}(\mathcal{A}_- \cap \overline{\mathcal{C}}_n)\\ &\quad + P_{X^nZ^n}(\mathcal{A}_0)).\end{aligned}$$

We use the following inequalities

$$P_{\mathcal{C}_n}(\mathcal{A}_+) \le e^{-b\sqrt{n}}, \tag{23}$$

$$P_{X^nZ^n}(\mathcal{A}_- \cap \overline{\mathcal{C}}_n) \le e^{-b\sqrt{n}}, \tag{24}$$

and

$$P_{X^nZ^n}(\mathcal{A}_0) \le \frac{2b}{\sqrt{2\pi\sigma}} + \frac{2C_1}{\sqrt{n}}\left(\frac{\rho}{\sigma}\right)^3, \tag{25}$$

where C_1 is a constant that does not depend on n and ρ is the third moment of $-\log P_{X|Z}(X|Z)$. We will prove these inequalities in Appendices B.1, B.2, and B.3 respectively.

From Eqs. (23)–(25) and the fact that $b > 0$ is arbitrary, we have

$$\begin{aligned}
&\liminf_{n\to\infty} \delta(P_{X^nZ^n}) \\
&\ge 1 - \limsup_{b\to 0} \limsup_{n\to\infty} [P_{\mathcal{C}_n}(\mathcal{A}_+) + \\
&\quad P_{X^nZ^n}(\mathcal{A}_- \cap \overline{\mathcal{C}}_n) + P_{X^nZ^n}(\mathcal{A}_0)] \\
&= 1.
\end{aligned}$$

Since the variational distance (divided by 2) is smaller than 1, we have the statement of theorem. □

5. Conclusion

In this paper, we showed that the encoders of (good) Slepian-Wolf codes cannot be used as functions for the secure privacy amplification in the sense of the variational distance criterion nor the divergence criterion. The consequence of our result is that we must use the privacy amplification not based on the Slepian-Wolf code (e.g. [2], [7], [12], [17]) if we want to employ the criteria other than weak one (the normalized divergence criterion).

Acknowledgment

The authors would like to thank Dr. Jun Muramatsu for comments. The first author also would like to thank Prof. Yasutada Oohama for his support. This research is partly supported by the Japan Society of Promotion of Science under Grants-in-Aid No. 00197137.

Appendix A: Proof of Theorem 4

In order to show a proof of Theorem 4, we need the following lemma [13] (see also [8]).

Lemma 16 For any Slepian-Wolf code $\Phi_n = (\phi_n, \psi_n)$, we have

$$\begin{aligned}
&\varepsilon(\Phi_n) \\
&\ge P_{X^nZ^n}\left(\left\{(x^n, z^n) : \right.\right. \\
&\qquad \left.\left. \log \frac{1}{P_{X^n|Z^n}(x^n|z^n)} \ge \alpha_n \right\}\right) - M_n e^{-\alpha_n},
\end{aligned}$$

where α_n is arbitrary real number. □

For arbitrarily fixed $\gamma > 0$, suppose that there exists a code sequence $\{\Phi_n\}$ that satisfies Eq. (8) and

$$\liminf_{n\to\infty} \frac{1}{\sqrt{n}} \log \frac{M_n}{e^{nH(X|Z)}} \le b - 2\gamma.$$

Then, there exists a increasing sequence $\{n_i\}_{i=1}^{\infty}$ such that

$$\frac{1}{\sqrt{n_i}} \log \frac{M_{n_i}}{e^{n_i H(X|Z)}} \le b - \gamma$$

for ever i.

By using Lemma 16 for $\alpha_{n_i} = \sqrt{n_i}b + n_i H(X|Z)$, we have

$$\begin{aligned}
&\varepsilon(\Phi_{n_i}) \\
&\ge P_{X^{n_i}Z^{n_i}}\left(\left\{(x^{n_i}, z^{n_i}) : \right.\right. \\
&\qquad \frac{1}{\sigma\sqrt{n_i}}\left(\log \frac{1}{P_{X^{n_i}|Z^{n_i}}(x^{n_i}|z^{n_i})} - n_i H(X|Z)\right) \\
&\qquad \left.\left. \ge \frac{b}{\sigma} \right\}\right) - e^{-\gamma\sqrt{n_i}}
\end{aligned}$$

for every i. By using the central limit theorem, we have

$$\begin{aligned}
\limsup_{n\to\infty} \varepsilon(\Phi_n) &\ge \limsup_{i\to\infty} \varepsilon(\Phi_{n_i}) \\
&\ge 1 - G\left(\frac{b}{\sigma}\right),
\end{aligned}$$

which contradict Eq. (8). Therefore, if the code sequence $\{\Phi_n\}$ satisfies Eq. (8), then it satisfies

$$\liminf_{n\to\infty} \frac{1}{\sqrt{n}} \log \frac{M_n}{e^{nH(X|Z)}} > b - 2\gamma.$$

Since $\gamma > 0$ is arbitrary, we have the assertion of the theorem. □

Appendix B

B.1 Proof of Eq. (23)

From the definitions of $P_{\mathcal{C}_n}$ and $\mathcal{A}_+$, we have

$$\begin{aligned}
P_{\mathcal{C}_n}(\mathcal{A}_+) &\le \sum_{(x^n,z^n)\in\mathcal{A}_+} \frac{1}{M_n} P_{Z^n}(z^n) \\
&\le \sum_{(x^n,z^n)\in\mathcal{A}_+} P_{X^nZ^n}(x^n, z^n) e^{-b\sqrt{n}} \\
&\le e^{-b\sqrt{n}}.
\end{aligned}$$

B.2 Proof of Eq. (24)

From the definitions of $P_{\mathcal{C}_n}$ and $\mathcal{A}_-$, we have

$$
\begin{aligned}
&P_{X^nZ^n}(\mathcal{A}_- \cap \overline{\mathcal{C}}_n) \\
&= \sum_{(x^n,z^n)\in\mathcal{A}_-\cap\overline{\mathcal{C}}_n} P_{X^nZ^n}(x^n,z^n) \\
&\le \sum_{(x^n,z^n)\in\mathcal{A}_-\cap\overline{\mathcal{C}}_n} \frac{1}{M_n} P_{Z^n}(z^n) e^{-b\sqrt{n}} \\
&= \sum_{(x^n,z^n)\in\mathcal{A}_-\cap\overline{\mathcal{C}}_n} P_{\mathcal{C}_n}(x^n,z^n) e^{-b\sqrt{n}} \\
&\le e^{-b\sqrt{n}}.
\end{aligned}
$$

B.3 Proof of Eq. (25)

To simplify the notation, we introduce the random variable

$$
W_n = \sum_{i=1}^{n} \log \frac{1}{P_{X|Z}(X_i|Z_i)}
$$

for $(X^n, Z^n) = ((X_1, Z_1), \ldots, (X_n, Z_n))$. Then, we can rewrite the left hand side of Eq. (25) as

$$
\begin{aligned}
&P_{X^nZ^n}(\mathcal{A}_0) \\
&= \Pr\{\log M_n - b\sqrt{n} \le W_n < \log M_n + b\sqrt{n}\} \\
&= \Pr\left\{ \frac{\log M_n - nH(X|Z)}{\sigma\sqrt{n}} - \frac{b}{\sigma} \right. \\
&\quad \le \frac{W_n - nH(X|Z)}{\sigma\sqrt{n}} \\
&\quad \left. < \frac{\log M_n - nH(X|Z)}{\sigma\sqrt{n}} + \frac{b}{\sigma} \right\} \\
&= \Pr\left\{ \frac{W_n - nH(X|Z)}{\sigma\sqrt{n}} \right. \\
&\quad \left. < \frac{\log M_n - nH(X|Z)}{\sigma\sqrt{n}} + \frac{b}{\sigma} \right\} \\
&- \Pr\left\{ \frac{W_n - nH(X|Z)}{\sigma\sqrt{n}} \right. \\
&\quad \left. < \frac{\log M_n - nH(X|Z)}{\sigma\sqrt{n}} - \frac{b}{\sigma} \right\}.
\end{aligned}
$$

By using the central limit theorem [16, Corollary 6], we have

$$
\begin{aligned}
&\Pr\left\{ \frac{W_n - nH(X|Z)}{\sigma\sqrt{n}} < \frac{\log M_n - nH(X|Z)}{\sigma\sqrt{n}} + \frac{b}{\sigma} \right\} \\
&\le \int_{-\infty}^{\frac{\log M_n - nH(X|Z)}{\sigma\sqrt{n}} + \frac{b}{\sigma}} g(u)du + \frac{C_1}{\sqrt{n}} \left(\frac{\rho}{\sigma}\right)^3
\end{aligned}
$$

and

$$
\begin{aligned}
&\Pr\left\{ \frac{W_n - nH(X|Z)}{\sigma\sqrt{n}} < \frac{\log M_n - nH(X|Z)}{\sigma\sqrt{n}} + \frac{b}{\sigma} \right\} \\
&\ge \int_{-\infty}^{\frac{\log M_n - nH(X|Z)}{\sigma\sqrt{n}} - \frac{b}{\sigma}} g(u)du - \frac{C_1}{\sqrt{n}} \left(\frac{\rho}{\sigma}\right)^3.
\end{aligned}
$$

Hence, we have

$$
P_{X^nZ^n}(\mathcal{A}_0) \le \int_{\frac{\log M_n - nH(X|Z)}{\sigma\sqrt{n}} - \frac{b}{\sigma}}^{\frac{\log M_n - nH(X|Z)}{\sigma\sqrt{n}} + \frac{b}{\sigma}} g(u)du + \frac{2C_1}{\sqrt{n}} \left(\frac{\rho}{\sigma}\right)^3.
$$

Since the interval of the integral is $\frac{2b}{\sigma}$ and the height of $g(u)$ is lower than 1, we have Eq. (25).

References

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–part 1: Secret sharing," IEEE Trans. Inform. Theory, vol.39, no.4, pp.1121–1132, 1993.

[2] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," IEEE Trans. on Inform. Theory, vol.41, no.6, pp.1915–1923, Nov. 1995.

[3] C.H. Bennett, G. Brassard, and J.M. Robert, "Privacy amplification by public discussion," SIAM Journal on Computing, vol.17, no.2, pp.210–229, Apr. 1988.

[4] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," Advances in Cryptology – EUROCRYPT '93, ed. T. Helleseth, Lecture Notes in Computer Science, vol.765, Lofthus, Norway, pp.410–423, 1994.

[5] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," Proc. 42nd IEEE Symposium on Foundations of Computer Science (FOCS), pp.136–145, Oct. 2001.

[6] T.M. Cover and J.A. Thomas, Elements of Information Theory, 2nd ed., John Wiley & Sons, 2006.

[7] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," IEEE Trans. Inform. Theory, vol.50, no.12, pp.3047–3061, December 2004.

[8] T.S. Han, Information-Spectrum Methods in Information Theory, Springer, 2003.

[9] T.S. Han, "Folklore in source coding: Information-spectrum approach," IEEE Trans. Inform. Theory, vol.51, no.2, pp.747–753, February 2005.

[10] M. Hayashi, "Second-order asymptotics in fixed-length source coding and intrinsic randomness," IEEE Trans. Inform. Theory, vol.54, no.10, pp.4619–4637, October 2008. arXiv:cs/0503089v2.

[11] U. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inform. Theory, vol.39, no.3, pp.733–742, May 1993.

[12] U. Maurer and S. Wolf, "Infromation-theoretic key agreement: From weak to strong secrecy for free," Advances in Cryptology – EUROCRYPT 2000, Lecture Notes in Computer Science, vol.1807, pp.351–368, Springer-Verlag, 2000.

[13] S. Miyake and F. Kanaya, "Coding theorems on correlated general sources," IEICE Trans. Fundamentals, vol.E78-A, no.9, pp.1063–1070, October 1995.

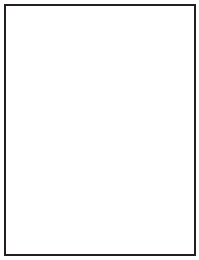
[14] J. Muramatsu, "Secret key agreement from correlated source outputs using low density parity check matrices," IEICE Trans. Fundamentals, vol.E89-A, no.7, pp.2036–2046, 2006. doi:10.1093/ietfec/e89-a.7.2036.

[15] M. Naito, S. Watanabe, R. Matsumoto, and T. Uyematsu, "Secret key agreement by soft-decision of signals in Gaussian Maurer's model," IEICE Trans. Fundamentals, vol.E92-A, no.2, February 2008. arXive:0804.2940v1.

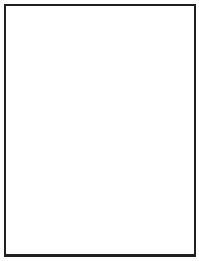
[16] M.M. Rao and R.J. Swift, Probability Theory with Applications, 2nd ed., Springer, 2005.

[17] R. Renner, Security of Quantum Key Distribution, Ph.D. thesis, Dipl. Phys. ETH, Switzerland, February 2005. arXiv:quant-ph/0512258, also available from International Journal of Quantum Information, vol. 6, no. 1, pp. 1–127, February 2008.

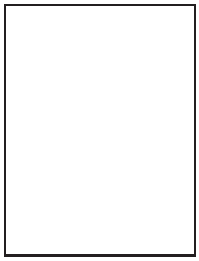
[18] R. Renner and S. Wolf, "Simple and tight bound for information reconciliation and privacy amplification," Advances in Cryptology – ASIACRYPT 2005, Lecture Notes in Computer Science, vol.3788, pp.199–216, Springer-Verlag, 2005.
[19] D. Slepian and J.K. Wolf, "Noiseless coding of correlated information sources," IEEE Trans. Inform. Theory, vol.19, no.4, pp.471–480, July 1973.



Shun Watanabe was born in Tokyo, Japan, on February 2, 1983. He received the B.E., M.E., and Ph.D. degrees from Tokyo Institute of Technology in 2005, 2007, and 2009 respectively. He is currently an Assistant Professor in the Department of Information Science and Intelligent Systems of Tokushima University. His current research interests are in the areas of information theory, quantum information theory, and quantum cryptography.



Ryutaroh Matsumoto was born in Nagoya, Japan, on November 29, 1973. He received the B.E. degree in computer science, the M.E. degree in information processing, and the Ph.D. degree in electrical and electronic engineering, all from Tokyo Institute of Technology, Japan, in 1996, 1998, 2001, respectively. He was an Assistant Professor from 2001 to 2004, and has been an Associate Professor since 2004 in the Department of Communications and Integrated Systems of Tokyo Institute of Technology. His research interest includes error-correcting codes, quantum information theory, and communication theory. Dr. Matsumoto received the Young Engineer Award from IEICE and the Ericsson Young Scientist Award from Ericsson Japan in 2001. He received the Best Paper Awards from IEICE in 2001 and 2008.



Tomohiko Uyematsu received the B.E., M.E. and Dr.Eng. degrees from Tokyo Institute of Technology in 1982, 1984 and 1988, respectively. From 1984 to 1992, he was with the Department of Electrical and Electronic Engineering of Tokyo Institute of Technology, first as research associate, next as lecturer, and lastly as associate professor. From 1992 to 1997, he was with School of Information Science of Japan Advanced Institute of Science and Technology as associate professor. Since 1997, he returned to Tokyo Institute of Technology as associate professor, and currently he is with the Department of Communications and Integrated Systems as professor. In 1992 and 1996, he was a visiting researcher at the Centre National de la Recherche Scientifique, France and Delft University of Technology, Netherlands, respectively. He received the Achievement Award in 2008, and the Best Paper Award in 1993, 1996, 2002 and 2007 both from IEICE. His current research interests are in the areas of information theory, especially Shannon theory and multi-terminal information theory. Dr. Uyematsu is a senior member of IEEE.